Hierarchical Video Surveillance Architecture - A Chassis for Video Big Data Analytics and Exploration

Sola O. Ajiboye*, Philip Birch, Christopher Chatwin, Rupert Young
Department of Engineering and Design
University of Sussex, Falmer-Brighton, United Kingdom

ABSTRACT

There is increasing reliance on video surveillance systems for systematic derivation, analysis and interpretation of the data needed for predicting, planning, evaluating and implementing public safety. This is evident from the massive number of surveillance cameras deployed across public locations. For example, in July 2013, the British Security Industry Association (BSIA) reported that over 4 million CCTV cameras had been installed in Britain alone. The BSIA also reveal that only 1.5% of these are state owned. In this paper, we propose a framework that allows access to data from privately owned cameras, with the aim of increasing the efficiency and accuracy of public safety planning, security activities, and decision support systems that are based on video integrated surveillance systems.

The accuracy of results obtained from government-owned public safety infrastructure would improve greatly if privately owned surveillance systems 'expose' relevant video-generated metadata events, such as triggered alerts and also permit query of a metadata repository. Subsequently, a police officer, for example, with an appropriate level of system permission can query unified video systems across a large geographical area such as a city or a country to predict the location of an interesting entity, such as a pedestrian or a vehicle. This becomes possible with our proposed novel hierarchical architecture, the Fused Video Surveillance Architecture (FVSA). At the high level, FVSA comprises of a hardware framework that is supported by a multi-layer abstraction software interface. It presents video surveillance systems as an adapted computational grid of intelligent services, which is integration-enabled to communicate with other compatible systems in the Internet of Things (IoT).

1 INTRODUCTION

Video surveillance systems capture and utilise data that will systematically predict, plan, evaluate and implement the protection of citizens and properties in both the private and public domains. In most cases, the cameras act as a physical deterrent but their data provide undeniable evidence in identifying and prosecuting offenders. It is common to install a significant number of surveillance systems in important public places. Because surveillance video often contains sensitive information and peoples' identity, it is imperative to manage and protect video surveillance systems and their data from unsolicited access.

Nonetheless, metadata generated from the surveillance systems can provide meaningful information without revealing the full identity of captured objects – metadata analytics is beneficial to all concerned parties. For organisations that have video surveillance systems in multiple locations, unifying their systems will reduce the total cost of ownership, improve scalability, and enhance maintenance since all systems have been unified into a single framework that can be managed from a single point. For public safety organisations such as the police, it provides a means for leveraging privately owned surveillance systems in the planning, prediction and investigation of crime.

In this paper, we propose a novel framework that supports automated generation of surveillance metadata and a controlled access to the metadata from any permitted system, with the aim of improving the accuracy of security alerts, public safety planning, and decision support systems that are based on state-owned video surveillance systems. Existing research into video metadata has focused on the generation and accessing of metadata by the administrative owner of the system. Our solution, the FVSA presents video surveillance systems as an adapted computational grid of intelligent services, which is integration-enabled to communicate with other compatible systems in the Internet of Things (IoT).

* sola.ajiboye@sussex.ac.uk

Now we will attempt to define computational grid, Internet of Things and, a unified system. Computational grid is a term used to describe a large-scale computing environment where high-powered intelligent devices and services (such as computers, storage services, sensor devices) are integrated to communicate for the purpose of leveraging their capability to mutually increase efficiency in terms of processing power, speed and input capacity. The computing resources of a computational grid are usually distributed across different geographic locations, with independent administrative ownership and management [2][3]. Internet of Things is a term that is popularly used to describe the ability to access features and administration of a digital device (or system) over the Internet - it describes virtual representation of uniquely identifiable devices in an internet-like architecture [4][5]. Lastly, this paper describes a unified system as the result when independent systems provide interfaces for sharing limited information. The administrative ownership and management of unified systems are independent.

A notable implementation of a computational grid based on the IoT is smart cities, which is a complex system comprising several unrelated lifeline services such as environmental information system, smart energy grid, travel information, waste management, urban planning, smart meters, emergency response, and smart events, which are being integrated across a common framework, (usually by implementing big data technology stack) [6] [7]. However, despite progressive trends of integrating systems across industries, as in smart city, video surveillance systems are still chiefly deployed and administered as standalone systems. Video data originates from each surveillance camera in large volumes without means to aggregately explore the embedded information. This is mainly because of complexities that are technical, financial, socio-cultural, security and ethically inclined, such as the following:

- Data protection – owners of video surveillance systems have a sense of responsibility to protect the privacy of the people captured in their data.
- Data ownership – fear of loss of full ownership and/or control over data if shared outside their own network facilities.
- Heavy cost and investment - surveillance systems were usually installed into the building structure; replacement may disrupt many other services, the financial cost can seem unrealistic or unreasonable.
- System incompatibility – based on manufacturer/vendor configuration and video encoding, video from each camera has a format that does not necessarily make it readily compatible with video from another camera.
- Unprofitable bandwidth usage – continuous and consecutive transmission of video by several cameras across the network, where many video frames may not contain interesting events.

This paper presents and describes how we resolve the complexities described above. The rest of this paper is organised as follows - section 2 reviews existing progress in improving accessibility to video surveillance data, focusing on current state of the art. Section 3 outlines our assumptions, goals and design considerations while section 4 describes our proposed architecture, the FVSA. In section 5, we suggest a sample implementation of the FVSA in a smart city network. The last section concludes this paper - we discussed relevance, strengths and envisaged challenges of our proposition and future direction for video surveillance systems based on our proposition.

2 RELATED WORK

High-end NVRs are already equipped with fast video processing capabilities. For example the BW® NVR5216-P (with 16 channels) runs a dual–core CPU and ample buffer memory allocation. It ships with surveillance applications and services including email service, intruder detection and alert generation but these NVRs are predominantly isolated systems, serving as an intelligent hub for all connected cameras. In our proposed model, multiple intelligent NVRs can be connected to jointly make up a surveillance network.

Intelligent data storage systems have been suggested for video surveillance systems with some capable of compressing the data before storing it [8]. In another work, Dey et al. proposed a solution capable of continuous I/O manipulations, read/write mix, random vs. sequential access with supporting variety of input sources [7]. Others have suggested storing video data in the cloud where growth becomes elastic and affordable [9]. However, while cloud storage is profitable and realistic solutions in most cases for extremely sensitive and/or massive data environments such as defence, cloud storage is not an option. As mentioned earlier, video from several surveillance cameras would consume massive bandwidth and

storage resources, and the video data can be highly sensitive. It would appear beneficial to persist video surveillance data within the local network with support for accessibility via a cloud based application layer.

Other notable works include metadata generation and analysis of the internal processing of surveillance systems. The works of Dian et. al. focused on the internal transactions in a video surveillance system including remote play, request and response flow [10]. Several works involved the systematic approaches to designing, deploying and implementing automated and event-based metadata from video surveillance systems including ontology and validation of events systems [11][12][13][14]. Metadata persists abstracted structures and content that users can query to retrieve meaningful information such as event detection and object tracking. Metadata can be queried independently of the video images - this can technically solve the problem of data protection.

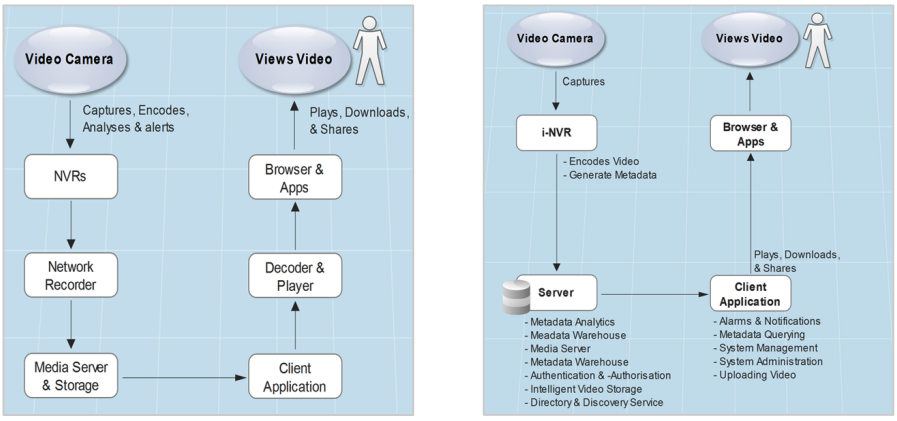
The FVSA is established on the reality of video metadata – with access authorisation implemented, surveillance systems can expose aspects of metadata. The exposed data can solely provide means for matching or comparing interesting events, making the data useful beyond the political and economic boundaries of the system owners and simultaneously protecting the privacy of the people in the video. A similar concept has been implemented in health informatics where patients' personal health records are de-identified and released for research – the de-identified data can be re-identified in the future for comparative analytics – the process is termed pseudonymisation [15].

3 DESIGN GOALS AND ASSUMPTIONS

We provide justification and reasoning for the design of the FVSA: in section 3.1, we briefly review the state of the art in video surveillance architectures; in sections 3.2, we discuss our aims and objectives while we discuss our design considerations and assumptions in section 3.3.

3.1 Current Systems

It is noted that current video surveillance architectures have been successful in the sense that they deter vandalism and provide a level of security to their administrative owners/managers [10] [16]. Figure 1a below is a common process flow in video surveillance systems. It shows that anyone with access to the computer screen or TV can view data from any camera on the network. A typical business model places a security officer in front of multiple screens where the officer attentively monitors video from the cameras in order to detect, investigate and raise alarms in the event of unwanted or unexpected scenes. Some of these systems provide the capability to watch real-time video from any camera on the network – permission to view the data is normally assumed since only authorised officers have physical access to the CCTV rooms. In recent years, as mentioned above in section 2, some of these systems are configurable to trigger alarms by sending email or SMS in the event of unwanted or unexpected events.



(a) (b)

Figure 1: Process flow for streaming video on a surveillance system (a) common process Flow in a current Surveillance Systems (b) process flow model in FVSA. In 1a, a user must be located in the control room to stream video from any camera on the network. In 1b, the user can stream video from any device running the system portal, which we described in section 4.

3.2 Design Goals

Our fundamental objective in this paper is to optimise the video surveillance systems, with a view to improving the quality and accuracy of information derived from them. The FVSA aims to analyse the events from video metadata as they are generated from cameras on the network. It provides authentication and authorisation to ensure that only permitted users can access the system where each user only has access as appropriate for his/her role. For example, while a security officer in a train station has been granted permission to view all surveillance data including real-time video, a police officer, may only have access to alerts that are triggered from the station. Similarly, a permitted police officer is conceptually aware of all video surveillance systems in town (through the directory server in section 4) and can seek permission to query them.

Figure 2 below is a map of the areas surrounding University of Sussex, UK. It is a page from the system's application portal, as seen by a city police officer using the FVSA. The map shows the FVSA deployed at four locations: a university campus, a stadium, Southern Water, and a train station. A city police officer has selected to view full details of the element of the Sussex FVSA system. An overview of the FVSA is provided in section 4 below.

A	University of Sussex	
	Number of cameras	100
	GID	uk-bn1-unisussex-falmer1
	Access-Level	Metadata-Query
	Full address	Sussex House
		Brighton, UK
		BN1 9RH
	Telephone number	+44 (0) 1273 606755
B	Falmer Train station	
C	Southern Water	
D	Amex Stadium (Football Club)	

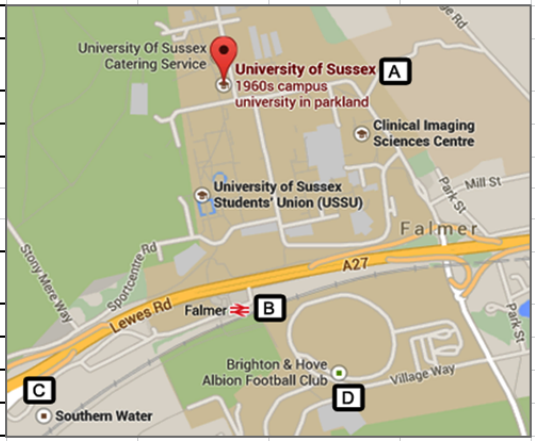


Figure 2: Topology of the video surveillance systems in a City – A Conceptual Police View

As noted earlier, surveillance data is the property and responsibility of the system owner. However a safety officer can be granted limited permission (time-limited or access-limited) to stream video data, which can help towards an investigation. Our proposal seems fit for purpose when deployed as a component of the bigger network such as a smart city. Our goals revolve around the need to optimise the video surveillance systems as technology advances towards aggregated analytics in the sense of the IoT, smart city, and hierarchical communications - we explain this further in section 5. Summarily, a video surveillance system based on FVSA will satisfy the following requirements:

- To reduce the cost of investigation – the police currently appeal for evidence from the public when investigating incidents. The FVSA can make data readily available for such investigations, so police can automatically query any 'open' video surveillance systems to build up evidence.
- To unify the data mining interface of independent video surveillance systems through a robust API.
- Surveillance system can interoperate in existing computational grids system, such as in a smart city or Cisco Service-Oriented Network Architecture (SONA) [17].
- Potential integration point for further sources of surveillance data such as satellite images, social media, which can provide useful information.
- To increase the accuracy of results obtained by public safety departments while the owners of independent surveillance system still protects their 'real' video data.
- Autonomous and continuous identification, tracking and investigation of objects from any camera on the network. And to generate statistical information for informed decision-making

- Apply a level of authorisation and authentication on the data to prevent fraudulent access.
- Perform high data compression on the video data so they are cheaper to store for a reasonable length of time.

3.3 Considerations and Assumptions

Our main assumptions are highlighted in Fig. 3 below:

- Public safety departments will be interested in using video from privately owned surveillance systems.
- We assume that current video systems can be preserved while the new architecture is implemented. However a new video surveillance system will benefit immensely from this new structure.
- We assume that owners or managers of CCTV systems will find our proposal more profitable and more beneficial.
- We assume cameras are unintelligent recording device; so all processing is achieved within the i-NVR.

4 THE FUSED VIDEO SURVEILLANCE ARCHITECTURE

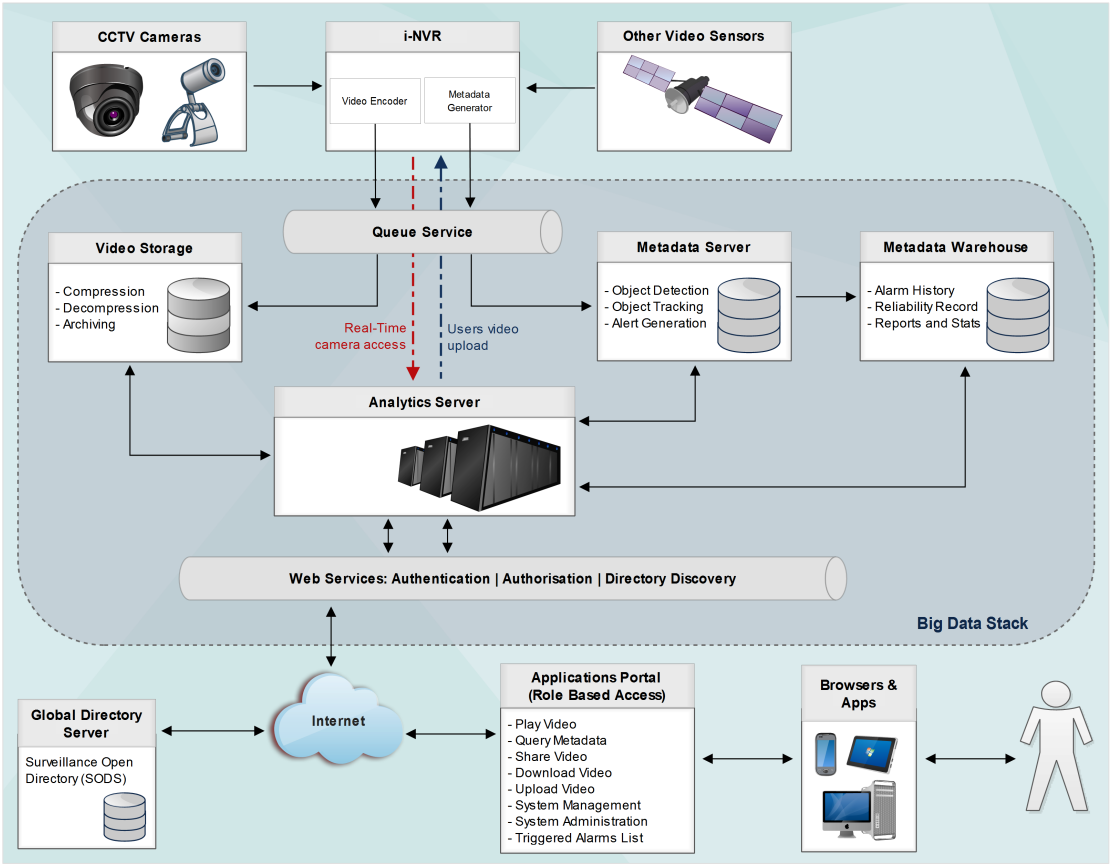


Figure 3: High Level Conceptual model of the FVSA, with system services in modular view. In practice, some of the modules depicted are merged – for example, the web services, metadata server (excluding storage), and queue services are all installed on the analytics server, which is ideally an implementation of a big data platform such as the Apache Hadoop platform.

4.1 Overview of the FVSA

Figure 3 above is a high-level architecture of the FVSA - it presents the following modules (i) cameras, (ii) intelligent Network Video Recorders (i-NVR), (iii) a queue service, (iv) a metadata server (MDS), (v) a metadata warehouse, (vi) an analytics server (vii) web services (viii) a global directory server (ix) user computer system. The operation of each module is explained below. It is worth noting that the framework described above can be set up flexibly, depending on the number of installed cameras and budget. If we consider the case of a small storeowner who requires only 1 camera – the camera can be equipped to perform the functions of an i-NVR in addition to capturing objects.

Camera Farm

The number of cameras on a system can be 1 or several thousand cameras. In small systems comprising only few cameras, an intelligent camera can perform the combined operations of a simple camera plus an i-NVR. However in large systems, all video processing can be achieved at the i-NVR, while unintelligent but high-resolution cameras can be used to capture data. System administrator can configure several cameras onto the same surveillance network even when they are deployed in different geographical locations, as in different cities/countries. For an organisation with branches across various cities and/or countries, the FVSA can be leveraged to administer all the CCTV systems from all location. This can be achieved by setting up the i-NVR hierarchically as described in the next section.

Analytics Server

The analytics server is responsible for analytics and exploration of the metadata, it is responsible for running queries, generating trends, alerts, predicting future events, based on learning of earlier events. This system is ideally an implementation of a reliable Big Data platform such as an Apache Hadoop stack. A Big Data platform can be deployed on commodity computers, so that the cost of hardware can be kept low for smaller systems, with ease of scalability for larger specs. It hosts compatible database engines/solution for storing and managing the metadata.

Storage (Video Storage, Metadata Database and Warehouse)

The intelligent video storage is empowered to transiently compress, decompress, and archive video data. It compresses data before persisting it for as long as configured but it can decompress and transmit a specified block of video on request. When the configured time lapses, the storage solution deletes old videos to provide space for more recent data.

Metadata contains information that was extracted from the video frames including camera identity, captured objects, and system owner. Data exploration and analytics are carried out on the metadata, so accuracy of results and reports depends on the quality of the metadata. The Metadata Server (MDS) must be included in any implementation of this architecture irrespective of the network size - it indexes and stores the metadata and is responsible for the following operations:

- Knowledge of all the cameras on the network (it receives data from them).
- Metadata is the main integrated resource in this architecture – all surveillance querying/investigation is carried out on the metadata through the API.
- It acts as network identifier as described in the next section

Intelligent Network Video Recorders (i-NVR)

In addition to connecting several cameras, the i-NVR encodes the video files and generates metadata before sending both to their storage solution(s).

Queuing System

On a large network with several cameras, bottlenecks and deadlock is expected when transmitting data. The queuing service is included to protect data integrity and manage deadlocks.

Web services

The web services, a RESTful service, manage all incoming and outgoing traffic to the system. These include system security in the sense of authentication, authorisation, trust and session management and system audit for establishing how data is being accessed. It also automatically discovers and registers or updates the directory service.

Directory Server

This service discovers, validates and organises a unique identity for all deployed instances of video surveillance systems that connect to it. The service is responsible for cataloguing available systems details, and contact details. The high-level functionality of this service is described in the next section. In practice, security firms and public safety departments such as the police will own and administer these services, and surveillance system owners can configure their systems as private (data will not be shared with any directory service) or public, where the system registers with the directory service.

User System

This comprises of a the user portal and devices such as a desktop computer, tablet, mobile phones and remote sensing devices such as satellite cameras, road traffic cameras, and mobile devices used by public safety officers. The portal provides an interface for capturing data from different devices and for requesting and responding to user actions such as uploading data, playing video and querying the metadata.

4.2 Hierarchies, System Scope and Visibility

A network architecture based on a flat design, which is one where all routing devices have full knowledge of the network, can only grow to a limited size – where the limitation is dictated by the capacity of the routers' memory size, processing power and transmission speeds. In order to build large networks where both inter-network and intra-network routing can scale efficiently, there is a need for hierarchical design [18]. A hierarchical network is partitioned into areas (or sub-networks) where each routing device only has full knowledge of its own local area. For each sub-network, there is an inter-network router, which has knowledge of neighbouring sub-networks. In practice, sub-networks are usually based on network ownership, geographical area covered or overall size of the network. Examples sub-networks are based on floor sub-networks, departmental networks, overall company networks, and city networks. Although these partitions are usually political and ownership defined, they enhance scalability, performance, security and efficiency of the bigger network.

The FVSA depicts video surveillance systems as a hierarchical system, where subsystem boundaries are based on administrative ownership and geographical location. Additionally, metadata servers (MDS) handle routing activities as discussed below. They are configurable as intra-system (local scope) or inter-system (global scope). An MDS in the local scope has full knowledge of the topological details of all the cameras in the system but does not have any knowledge about any external camera. However in the global scope, an MDS provides connectivity to an external surveillance system through the Directory service as described below.

In Figure 4 below, an L-MDS only has knowledge of cameras that directly connect to it, and those that connect through an i-NVR and those that are connected to neighbour L-MDSs. Any G-MDS knows how to contact any other G-MDS that is connected to the directory server, however the level of access or visibility depends on the role of the user. For example, in Figure 4, the various L-MDS in the city mall system represents various FVSA systems in the mall, where different shops own and independently manage their own surveillance system. The mall's authority however provides a G-MDS, which every shop can connect to. The mall authority manages the G-MDS and at the same time, the G-MDS can provide connectivity to the city police. With this in place, the mall authority can provide evidence of events without the police physically visiting the mall.

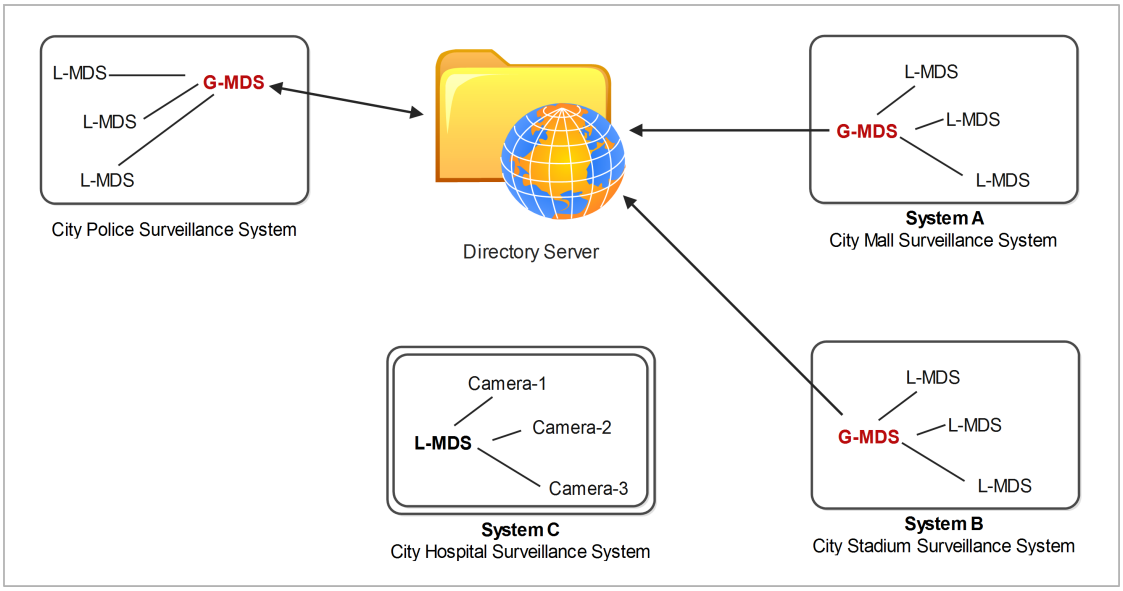


Figure 4: Global and local scope of the MDS – the G-MDS connects to other G-MDS while each L-MDS can only administer cameras within its own system boundary. The MDS in system C, which depicts the city hospital surveillance system, is configured for local use only. The cameras and data in system C are therefore not available outside the hospital network.

Authorisation and Resource Visibility

Any information destined outside the system has to be initiated by a G-MDS, provided the user meets authentication and authorisation requirements. Only the local administrator has full authorisation on all system services. Any user that is not local to the system has to be granted authorisation to use a specific service. For example, by default, a police office can view a system overview of any connected surveillance system but to play video or query such a system, the system owner must first authorise the access. In Table 1 below, it is noted that all external users are not allowed access to the service but public safety officers such as the police may be given authorisation to access some services.

Table 1: Visibility and authorization of system services.

Services in system A (Figure 4 above)	**An admin of system A**	**An admin of system B**	**A city police officer**
Views system overview: cameras, and contact information.	Yes	No	Yes
Plays recorded video.	Yes	No	No, unless permitted by system A.
Queries System	Yes	No	No, unless permitted by system A.
Receives feeds and alerts	Yes	No	No, unless permitted by system A.
Configures/updates system or cameras.	Yes	No	No

5 PROTOTYPE AND RELEVANCE

Figure 5 below shows the surveillance system in a smart city network - it is noted that each FVSA layer is relevant to a layer in other grid computing platforms, such as smart cities. The layers (or hierarchies) in this view of the architecture fall into either hardware domain (physical and network layers) or software domain (services and application layers). The physical layer comprises all the devices that capture video such as cameras. The network layer includes all network and switching devices such as the routers, MDS, and mobile antennas. The services layer comprises of network-based data solutions and service APIs such as cloud storage. The application layer comprises of client applications and services through which users interact with the system such as video player and query browser.

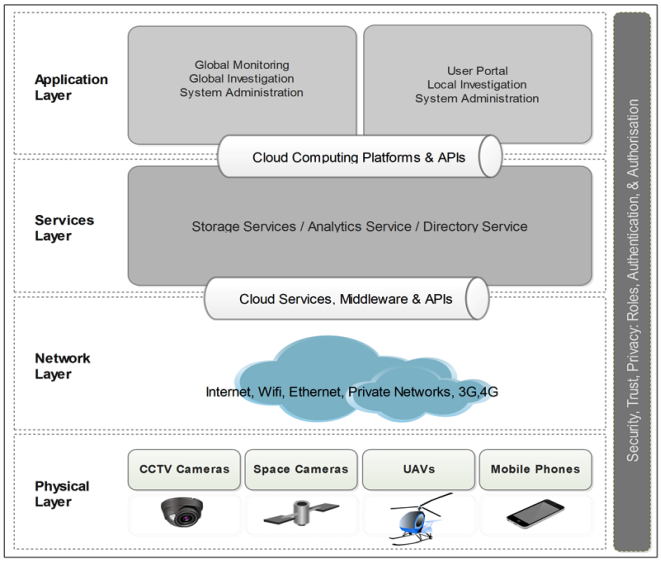


Figure 5 Layered architecture of the FVSA showing its relevance to other IoT compatible architecture (based on earlier works such as [4] [5] [6]) – a view of the hierarchical design where each layer is depicted as a layer of the overall system architecture. Physical and Network layers are hardware based while Application and Services layers are software implementation.

6 CONCLUSION

We have offered solutions for the problems described and highlight major areas that are still work in progress. The solutions proposed by the FVSA include unification of independent surveillance systems. As described in section 4, each implementation of the FVSA is independent while several instances can integrate to form a larger system (or a unified system), such as a city's surveillance system. The same section also introduced the directory server, which is the integration catalogue for unifying the systems. With this in place, section 3 introduced how authorised public safety officers can 'browse' all connected surveillance systems within their jurisdiction, with latent ability to review alerts and video from any camera. In section 5, we demonstrate FVSA's compatibility with other hierarchical network solutions such as a smart city.

Ultimately, we suggest a hierarchical design and a high-level configuration for video surveillance devices and services, making it possible to approach video networks in layers such as internal system (local) or external system (global). Hierarchical design is an approach engineers employ to abstract complex multifaceted problems/requirements into granular manageable subsystems. The framework of our solution is compatible with the hierarchical structure of computer networks and emerging technologies.

REFERENCES

[1] S. Adcock and P. Norstrom, "Just 1 in 70 CCTV Cameras are State-Owned: Survey Revelation by the British Security Industry Association (BSIA)," *Press Conference, London*, 2013. [Online]. Available: http://www.bsia.co.uk/home/bsia-cctv-number-of-cameras-in-uk. [Accessed: 17-Sep-2014].

[2] S. Zikos and H. D. Karatza, "Clairvoyant site allocation of jobs with highly variable service demands in a computational grid," in *2010 IEEE International Symposium on Parallel & Distributed Processing, Workshops and Phd Forum (IPDPSW)*, 2010, pp. 1–8.

[3] A. Pradesh, "A Novel Fault-tolerant Task Scheduling Algorithm for Computational Grids," in *2013 15th International Conference on Advanced Computing Technologies (ICACT)*, 2013, pp. 1–6.

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[5] S. Fang, L. Da Xu, S. Member, Y. Zhu, J. Ahati, H. Pei, J. Yan, and Z. Liu, "An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things," in *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, 2014, vol. 10, no. 2, pp. 1596–1605.

[6] C. Tao, X. Ling, S. Guofeng, Y. Hongyong, and H. Quanyi, "Architecture for Monitoring Urban Infrastructure and Analysis Method for a Smart-Safe City," in *2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, 2014, pp. 151–154.

[7] S. Dey, A. Chakraborty, S. Naskar, and P. Misra, "Smart city surveillance: Leveraging benefits of cloud data stores," in *goSMART 2012, Clearwater*, 2012, no. 978–1–4673–2130–3, pp. 868–876.

[8] R. Xue, Z.-S. Wu, and A.-N. Bai, "Application of Cloud Storage in Traffic Video Detection," *2011 Seventh Int. Conf. Comput. Intell. Secur.*, pp. 1294–1297, Dec. 2011.

[9] Y. Huo, H. Wang, and L. Hu, "A Cloud Storage Architecture Model for Data- Intensive Applications," in *2011 International Conference on Computer and Management (CAMAN)*, 2011, no. 61073009, pp. 26–29.

[10] D. Chu, C. Jiang, Z. Hao, and W. Jiang, "The Design and Implementation of Video Surveillance System Based on H.264, SIP, RTP/RTCP and RTSP," in *2013 Sixth International Symposium on Computational Intelligence and Design*, 2013, vol. 2, pp. 39–43.

[11] J. R. Smith, R. J. Alexandre, J. Hobbs, and R. C. Bolles, "VERL : An Ontology Framework for Representing and Annotating Video Events," *MultiMedia, IEEE*, vol. 12, no. 4, pp. 76–86, 2005.

[12] R. Nevatia, J. Hobbs, B. Bolles, and M. Rey, "An Ontology for Video Event Representation," in *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW'04)*, 2004.

[13] H. Zhou and G. K. H. Pang, "Metadata extraction and organization for intelligent video surveillance system," in *International Conference on Mechatronics and Automation (ICMA), 2010*, 2010, pp. 489–494.

[14] H. Zhou, L. Jia, and Y. Qin, "Metadata Specification of Railway Video Information and its application in Video Monitoring System for Qinghai-Tibet Railway," in *International Symposium on Computer Network and Multimedia Technology, 2009. CNMT 2009.*, 2009, no. 600332020.

[15] R. Rawassizadeh, J. Heurix, S. Khosravipour, and a. M. Tjoa, "LiDSec- A Lightweight Pseudonymization Approach for Privacy-Preserving Publishing of Textual Personal Information," in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011, pp. 603–608.

[16] X. Zhu, H. Deng, Z. Chen, and H. Yang, "Design of Large-Scale Video Surveillance System Based on P2P Streaming," in *2011 3rd International Workshop on Intelligent Systems and Applications*, 2011, pp. 1–4.

[17] W. Paper, "The Cisco SONA Architectural Model in Unified Communications: A Solid Foundation for the Collaborative Innovative Enterprise," 2008. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/branch/White_paper_C11-473760.html.

[18] R. Perlman and C. Kaufman, "Hierarchical networks with Byzantine Robustness," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, 2011, pp. 1–11.